UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/046,224	01/16/2002	Mototsugu Nishioka	500.41092X00	4402

24956 7590 05/17/2005

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 DIAGONAL ROAD
SUITE 370
ALEXANDRIA, VA 22314

EXAMINER
CERVETTI, DAVID GARCIA

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 05/17/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/046,224	**Applicant(s)** NISHIOKA ET AL.	
	Examiner David G. Cervetti	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 January 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☒ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *2/26/02*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

The listing of references in the specification is not a proper information disclosure statement. 37 CFR 1.98(b) requires a list of all patents, publications, or other information submitted for consideration by the Office, and MPEP § 609 A(1) states, "the list may not be incorporated into the specification but must be submitted in a separate paper." Therefore, unless the references have been cited by the examiner on form PTO-892, they have not been considered.

Claim Objections

Claim 1 is objected to because of the following informalities: "(multiplicative)", "(the order of G)", "(where α..)". The parenthesis should be removed for the limitation to be given patentable weight. Appropriate correction is required.

Claim 2 is objected to because of the following informalities: "(q is a prime factor…)", "(10^{k1+k2} ….<p)", "($|\alpha_1| = k_1$, $|\alpha_2| = k_2$)", "($|m| = k_3$ where…)". The parenthesis should be removed for the limitation to be given patentable weight. Appropriate correction is required.

Claim 6 is objected to because of the following informalities: "(symmetric cryptographic function E and key data K" (page 39, line 4).

Claim 18 is objected to because of the following informalities: "$E_{pk}(.)$: (asymmetric cryptography) encipher function" (page 47, line 10). The meaning of $E_{pk}(.)$ is not clear.

Please note that this is not a complete list of occurrences.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 14 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 14 recites the limitation "transmitting the ciphertext (u_1, u_2, v, **C**)" in page 45, line 16. There is insufficient antecedent basis for this limitation in the claim.

Claim 18 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 18 recites the limitation "where the group G is a partial group of the group **G'**" in page 47, line 11. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cramer et al. (US Patent Number: 6,697,488).

Regarding claim 1, Cramer et al. teach a public-key cryptographic scheme comprising: a key generation step of generating a secret-key:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in Z_q$ (column 7, lines 10-19), and
- a public-key:
    - o G, G': finite (multiplicative) group $G \subseteq G'$,
    - o q: prime number (the order of G),
    - o $g_1, g_2 \in G$ (column 6, lines 65-67, column 7, lines 1-10),
    - o $c= g_1\hat{}x_1\, g_2\hat{}x_2$, $d_1= g_1\hat{}y_{11}\, g_2\hat{}y_{12}$, $d_2= g_1\hat{}y_{21}\, g_2\hat{}y_{22}$, $h= g_1\hat{}z$,
    - o $\pi : X_1 \text{ x } X_2 \text{ x } M \rightarrow G'$: one-to-one mapping
    - o $\pi^{-1} : Im(\pi) \rightarrow X_1 \text{ x } X_2 \text{ x } M$ (column 7, lines 20-27)
- where the group G is a partial group of the group G', X_1 and X_2 are an infinite set of positive integers which satisfy: $\alpha_1 \,||\, \alpha_2<q$ (for every $\alpha_1 \in X_1$, for every $\alpha_2 \in X_2$) where M is a plaintext space;

- a cipher-text generation and transmission step of selecting random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in Z_q$ for a plaintext m (m ∈ M), calculating: u_1=g_1^r, u_2=g_2^r, e=π(α_1, α_2, m)h^r, v=g_1^ α_1 c^r d_1^ αr d_2^ mr (column 7, lines 55-67, column 8, lines 1-22) where α = α_1 || α_2 and transmitting (u_1, u_2, e, v) as a ciphertext (column 8, lines 24-35); and
- a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α_1', α_2', m' ($\alpha_1' \in X_1$, $\alpha_2' \in X_2$, m'∈ M) which satisfy: π (α_1', α_2', m') = e/(u_1^z) (column 8, lines 36-67, column 9,lines 1-67, column 10, lines 1-67)
- and if the following is satisfied:

  (g_1^α_1')(u_1^(x_1+ α'y_{11}+m'y_{21}))(u_2^(x_2+ α'y_{12}+m'y_{22}))=v

  outputting m' as the deciphered results (where α' = α_1' || α_2', whereas if not satisfied, outputting as the decipher results the effect that the received cipher-text is rejected (column 8, lines 36-67).

Cramer et al. disclose generating a secret-key using five exponent numbers (x_1, x_2, y_1, y_2, $z \in Z_q$), generating a public-key, and transmitting a cipher-text (u_1, u_2, e, v). Furthermore, Cramer et al. teach generating extended private key and public key (column 4, lines 19-45). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate the secret key by modifying Cramer et al.'s generating step. One of ordinary skill in the art would have been motivated to do so to increase the security of the cryptographic scheme (Cramer et al., column 4, lines 19-67).

Regarding claim 2, Cramer et al. teach a public-key cryptographic scheme comprising: a key generation step of generating a secret-key:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in Z_q$ (column 7, lines 10-19), and
- a public-key:
    - o p, q: prime number (q is a prime factor of p-1),
    - o $g_1, g_2 \in Z_p$: $\mathrm{ord}_p(g_1) = \mathrm{ord}_p(g_2) = q$ (column 6, lines 65-67, column 7, lines 1-10),
    - o $c = g_1$^$x_1\, g_2$^x_2 mod p, $d_1 = g_1$^$y_{11}\, g_2$^y_{12} mod p, $d_2 = g_1$^$y_{21}\, g_2$^y_{22} mod p, $h = g_1$^z mod p,
    - o k_1 , k_2 , k_3 : positive constant ($10^{k1+k2} < q$, $10^{k3} < q$, $10^{k1+k2+k3} < p$) (column 7, lines 20-27)
- a cipher-text generation and transmission step of selecting random numbers $\alpha = \alpha_1 \| \alpha_2$ ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$) for a plaintext m ($|m| = k_3$ where $|x|$ is the number of digits of x), calculating: $m = \alpha \| K$
- selecting a random number $r \in Z_q$, calculating: $u_1 = g_1^r$ mod p, $u_2 = g_2^r$ mod p, $e = m\, h^r$ mod p, $v = g_1$^ $\alpha_1\, c^r\ d_1$^ $\alpha r\ d_2$^ mr mod p and transmitting (u_1, u_2, e, v) as a ciphertext (column 8, lines 24-35); and
- a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α_1', α_2', m' ($|\alpha_1'| = k_1$, $|\alpha_2'| = k_2$, $|m'| = k_3$) which satisfy: $\alpha_1' \| \alpha_2' \| m' = e/(u_1$^z) mod p (column 8, lines 36-67, column 9,lines 1-67, column 10, lines 1-67)

- and if the following is satisfied:

  $(g_1{}^\wedge\alpha_1')(u_1{}^\wedge(x_1+ \alpha' y_{11}+m' y_{21}))(u_2{}^\wedge(x_2+ \alpha' y_{12}+m' y_{22}))\equiv v \text{ (mod p)}$

  outputting m' as the deciphered results (where $\alpha' = \alpha_1' \,||\, \alpha_2'$, whereas if not satisfied, outputting as the decipher results the effect that the received cipher-text is rejected (column 8, lines 36-67).

Cramer et al. disclose generating a secret-key using five exponent numbers (x_1, x_2, y_1, y_2, $z \in Z_q$), generating a public-key, and transmitting a cipher-text (u_1, u_2, e, v). Furthermore, Cramer et al. teach generating extended private key and public key (column 4, lines 19-45). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate the secret key by modifying Cramer et al.'s generating step. One of ordinary skill in the art would have been motivated to do so to increase the security of the cryptographic scheme (Cramer et al., column 4, lines 19-67).

Regarding claim 3, Cramer et al. do not disclose expressly wherein the public-key is generated by a receiver and is made public. However, Examiner takes Official Notice that having a receiver generating a public-key and making it public is conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to have a receiver generate a public-key and make it public since Examiner takes Official Notice that having a receiver generating a public-key and making it public is conventional and well known.

Regarding claim 4, Cramer et al. teach wherein in said ciphertext transmission step, the random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, and $r \in Z_q$ are selected beforehand and the following is calculated and stored beforehand: $u_1=g_1^r$, $u_2=g_2^r$, h^r, g_1^α_1 c^r d_1^αr (column 7, lines 40-67, column 8, lines 1-22).

Regarding claim 5, Cramer et al. teach wherein in said ciphertext transmission step, the random numbers α_1, α_2 ($|\alpha_1|= k_1$, $|\alpha_2|= k_2$) are selected beforehand and the following is calculated and stored beforehand: $u_1=g_1^r \bmod p$, $u_2=g_2^r \bmod p$, $h^r \bmod p$, g_1^α_1 c^r d_1^αr mod p (column 7, lines 40-67, column 8, lines 1-22).

Regarding claim 6, Cramer et al. teach a cryptographic communication method comprising: a key generation step of generating a secret-key:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in Z_q$ (column 7, lines 10-19), and
- a public-key:
  - G, G': finite (multiplicative) group $G \subseteq G'$,
  - q: prime number (the order of G),
  - $g_1, g_2 \in G$ (column 6, lines 65-67, column 7, lines 1-10),
  - c= g_1^x_1 g_2^x_2, d_1= g_1^y_{11} g_2^y_{12}, d_2= g_1^y_{21} g_2^y_{22}, h= g_1^z,
  - $\pi : X_1 \times X_2 \times M \rightarrow G'$: one-to-one mapping
  - $\pi^{-1} : \mathrm{Im}(\pi) \rightarrow X_1 \times X_2 \times M$ (column 7, lines 20-27)
  - E : symmetric encipher function (column 12, lines 1-35)
- where the group G is a partial group of the group G', X_1 and X_2 are an infinite set of positive integers which satisfy: $\alpha_1 \,||\, \alpha_2 < q$ (for every $\alpha_1 \in X_1$, for every $\alpha_2 \in X_2$) where M is a plaintext space;

- a cipher-text generation and transmission step of selecting random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in Z_q$ for key data K ($K \in M$), calculating: $u_1=g_1{\wedge}r$, $u_2=g_2{\wedge}r$, $e=\pi(\alpha_1, \alpha_2, K)h^r$, $v=g_1{\wedge}\, \alpha_1 c^r\ d_1{\wedge}\, \alpha r\ d_2{\wedge}\, Kr$ (column 7, lines 55-67, column 8, lines 1-22) where $\alpha = \alpha_1 \| \alpha_2$, generating a ciphertext C of transmission data m by: $C = E_K(m)$ (column 12, lines 1-35) by using a symmetric cryptographic function E and key data K, and transmitting (u_1, u_2, e, v, C) as the ciphertext (column 8, lines 24-35); and
- a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α_1', α_2', K' ($\alpha_1' \in X_1$, $\alpha_2' \in X_2$, $K' \in M$) which satisfy: $\pi\ (\alpha_1' \| \alpha_2' \| K') = e/(u_1{\wedge}z)$ (column 8, lines 36-67, column 9,lines 1-67, column 10, lines 1-67)
- and if the following is satisfied: $(g_1{\wedge}\alpha_1')(u_1{\wedge}(x_1+ \alpha' y_{11}+K' y_{21}))(u_2{\wedge}(x_2+ \alpha' y_{12}+K' y_{22}))=v$ where $\alpha' = \alpha_1' \| \alpha_2'$, executing a decipher process by: $m=D_{K'}(C)$ outputting deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received cipher- text is rejected (column 8, lines 36-67).

Cramer et al. disclose generating a secret-key using five exponent numbers (x_1, x_2, y_1, y_2, $z \in Z_q$), generating a public-key, and transmitting a cipher-text (u_1, u_2, e, v). Furthermore, Cramer et al. teach generating extended private key and public key (column 4, lines 19-45). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate the secret key by modifying Cramer et al.'s generating step. One of ordinary skill in the art would have been motivated to do so to increase the security of the cryptographic scheme (Cramer et al., column 4, lines 19-67).

Regarding claim 7, Cramer et al. teach wherein the ciphertext C is generated by: $C = E_K(f(\alpha_1,\alpha_2) \,||\, m)$ by using a symmetric cryptographic function E (column 12, lines 1-35), the key data K and a publicized proper function f, it is checked whether the following is satisfied:

$(g_1{}^\wedge\alpha_1')(u_1{}^\wedge(x_1+ \alpha'y_{11}+K'y_{21}))(u_2{}^\wedge(x_2+ \alpha'y_{12}+K'y_{22}))=v$

$f(\alpha_1',\alpha_2') = [D_{K'}(C)]^K$

where f outputs a value of k bits and $[x]^K$ indicates the upper k bits of x, and if the check passes, a decipher process is executed by: $m= [D_{K'}(C)]^{-K}$ where $[x]^{-k}$ indicates a bit train with the upper k bits of x being removed (column 8, lines 36-67, column 12, lines 1-35).

Regarding claim 8, Cramer et al. teach a cryptographic communication method comprising: a key generation step of generating a secret-key:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in Z_q$ (column 7, lines 10-19), and
- a public-key:

- p, q: prime number (q is a prime factor of p-1),
- $g_1, g_2 \in \mathbb{Z}_p$: $\mathrm{ord}_p\,(g_1) = \mathrm{ord}_p\,(g_2) = q$ (column 6, lines 65-67, column 7, lines 1-10),
- $c= g_1{}^\wedge x_1\, g_2{}^\wedge x_2 \bmod p$, $d_1= g_1{}^\wedge y_{11}\, g_2{}^\wedge y_{12} \bmod p$, $d_2= g_1{}^\wedge y_{21}\, g_2{}^\wedge y_{22} \bmod p$, $h= g_1{}^\wedge z \bmod p$,
- k_1 , k_2 , k_3 : positive constant ($10^{k1+k2} < q$, $10^{k3} < q$, $10^{k1+k2+k3} < p$) (column 7, lines 20-27)
- E : symmetric encipher function (column 12, lines 1-35)

- a cipher-text generation and transmission step of selecting random numbers $\alpha = \alpha_1 \,||\, \alpha_2$ ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$) for key data K ($|K| = k_3$ where $|x|$ is the number of digits of x), calculating $m = \alpha||K$
- selecting a random number $r \in Z_{q,}$ calculating:

  $u_1= g_1{}^r \bmod p$, $u_2= g_2{}^r \bmod p$, $e= m\, h^r \bmod p$, $v=g_1{}^\wedge\ \alpha_1\, c^r\ \ d_1{}^\wedge\, \alpha r\ d_2{}^\wedge\, Kr \bmod p$ and generating a ciphertext C of transmission data by: $C = E_K\,(m)$ (column 12, lines 1-35) by using a symmetric cryptographic function E and the key data K, and transmitting (u_1, u_2, e, v, C) as the ciphertext (column 8, lines 24-35); and
- a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α_1', α_2', K' ($|\alpha_1'|=k_1$, $|\alpha_2'|=k_2$, $|K'|= k_3$) which satisfy: $\alpha_1'||\ \alpha_2'||\ K' = e/(u_1{}^\wedge z) \bmod p$ (column 8, lines 36-67, column 9,lines 1-67, column 10, lines 1-67)

- and if the following is satisfied: $(g_1\hat{}\alpha_1')(u_1\hat{}(x_1+\alpha'y_{11}+K'y_{21}))(u_2\hat{}(x_2+\alpha'y_{12}+K'y_{22}))=v \pmod p$ where $\alpha' = \alpha_1' \mid\mid \alpha_2'$, executing a decipher process by: $m=D_{K'}(C)$ outputting deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received cipher- text is rejected (column 8, lines 36-67).

Cramer et al. disclose generating a secret-key using five exponent numbers (x_1, x_2, y_1, y_2, $z \in Z_q$), generating a public-key, and transmitting a cipher-text (u_1, u_2, e, v). Furthermore, Cramer et al. teach generating extended private key and public key (column 4, lines 19-45). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate the secret key by modifying Cramer et al.'s generating step. One of ordinary skill in the art would have been motivated to do so to increase the security of the cryptographic scheme (Cramer et al., column 4, lines 19-67).

Regarding claim 9, Cramer et al. teach wherein the ciphertext C is generated by: $C = E_K(f(\alpha_1,\alpha_2) \mid\mid m)$ by using a symmetric cryptographic function E (column 12, lines 1-35), the key data K and a publicized proper function f, it is checked whether the following is satisfied:

$(g_1\hat{}\alpha_1')(u_1\hat{}(x_1+\alpha'y_{11}+K'y_{21}))(u_2\hat{}(x_2+\alpha'y_{12}+K'y_{22}))=v \pmod p$,

$f(\alpha_1',\alpha_2') = [D_{K'}(C)]^k$

where f outputs a value of k bits and $[x]^k$ indicates the upper k bits of x, and if the check passes, a decipher process is executed by: m= $[D_{K'}(C)]^{-K}$ where $[x]^{-k}$ indicates a bit train with the upper k bits of x being removed (column 8, lines 36-67, column 12, lines 1-35).

Regarding claim 10, Cramer et al. do not disclose expressly wherein the public-key is generated by a receiver and is made public. However, Examiner takes Official Notice that having a receiver generating a public-key and making it public is conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to have a receiver generate a public-key and make it public since Examiner takes Official Notice that having a receiver generating a public-key and making it public is conventional and well known.

Regarding claim 11, Cramer et al. teach wherein in said ciphertext transmission step, the random numbers α_1, α_2 ($\alpha_1 \in X_1$, $\alpha_2 \in X_2$) and $r \in Z_q$ are selected beforehand and the following is calculated and stored beforehand: $u_1=g_1^r$, $u_2=g_2^r$, h^r, g_1^α_1 c^r d_1^αr (column 7, lines 40-67, column 8, lines 1-22).

Regarding claim 12, Cramer et al. teach wherein in said ciphertext transmission step, the random numbers α_1, α_2 ($|\alpha_1|= k_1$, $|\alpha_2|= k_2$) and $r \in Z_q$ are selected beforehand and the following is calculated and stored beforehand: $u_1=g_1^r$ mod p, $u_2=g_2^r$ mod p, h^rmod p, g_1^α_1 c^r d_1^αr mod p (column 7, lines 40-67, column 8, lines 1-22).

Regarding claim 13, Cramer et al. teach a cryptographic communication method comprising: a key generation step of generating a secret-key:

- $x_1, x_2, y_1, y_2, z \in Z_q$ (column 7, lines 10-19), and

- a public-key:
  - G, G': finite (multiplicative) group $G \subseteq G'$,
  - q: prime number (the order of G),
  - $g_1, g_2 \in G$ (column 6, lines 65-67, column 7, lines 1-10),
  - $c= g_1{}^\wedge x_1 g_2{}^\wedge x_2$, $d = g_1{}^\wedge y_1 g_2{}^\wedge y_2$, $h= g_1^z$,
  - $\pi : X_1 \times X_2 \times M \rightarrow \mathrm{Dom}(E)$: one-to-one mapping ($\mathrm{Dom}(E)$ is the domain of the function E)
  - $\pi^{-1} : \mathrm{Im}(\pi) \rightarrow X_1 \times X_2 \times M$ (column 7, lines 20-27)
  - H : hash function (column 12, lines 1-35)
  - E : symmetric encipher function (column 12, lines 1-35)
- where the group G is a partial group of the group G', X_1 and X_2 are an infinite set of positive integers which satisfy: $\alpha_1 \| \alpha_2 < q$ (for every $\alpha_1 \in X_1$, for every $\alpha_2 \in X_2$) where M is a plaintext space;
- a cipher-text generation and transmission step of selecting random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in Z_q$, calculating: $u_1=g_1^r$, $u_2=g_2^r$, $v=g_1{}^\wedge \alpha_1 c^r d^{\alpha r}$, $K = H(h^r)$ (column 7, lines 55-67, column 8, lines 1-22) where $\alpha = \alpha_1 \| \alpha_2$, generating a ciphertext C of transmission data m by: $C = E_K(\pi(\alpha_1, \alpha_2, m))$ (column 12, lines 1-35) by using a symmetric cryptographic function E; and transmitting (u_1, u_2, v, C) as the ciphertext (column 8, lines 24-35); and

- a ciphertext reception and decipher step of calculating K' = $H(u_1^z)$ by using the secret key, calculating from the received ciphertext, α_1', α_2', (where $\alpha_1' \in X_1$, $\alpha_2' \in X_2$) which satisfy: $\pi(\alpha_1', \alpha_2', m') = D_{K'}(C)$ (column 8, lines 36-67, column 9,lines 1-67, column 10, lines 1-67)
- and if the following is satisfied: $(g_1\wedge\alpha_1')(u_1\wedge(x_1+ \alpha' y_1))(u_2\wedge(x_2+ \alpha' y_2))=v$, where $\alpha' = \alpha_1' \| \alpha_2'$, outputting m' as the deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received cipher- text is rejected (column 8, lines 36-67).

Cramer et al. disclose generating a secret-key using five exponent numbers (x_1, x_2, y_1, y_2, $z \in Z_q$), generating a public-key, and transmitting a cipher-text (u_1, u_2, e, v). Furthermore, Cramer et al. teach generating extended private key and public key (column 4, lines 19-45). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate the secret key by modifying Cramer et al.'s generating step. One of ordinary skill in the art would have been motivated to do so to increase the security of the cryptographic scheme (Cramer et al., column 4, lines 19-67).

Regarding claim 14, Cramer et al. teach a cryptographic communication method comprising: a key generation step of generating a secret-key:

- x_1, x_2, y_1, y_2, $z \in Z_q$ (column 7, lines 10-19), and
- a public-key:
  - p, q: prime number (q is a prime factor of p-1),

- $g_1, g_2 \in Z_p$: $ord_p(g_1) = ord_p(g_2) = q$ (column 6, lines 65-67, column 7, lines 1-10),
- $c = g_1$^x_1 g_2^x_2 mod p, $d = g_1$^y_1 g_2^y_2 mod p, $h = g_1^z$ mod p,
- k_1 , k_2 , k_3 : positive constant ($10^{k1+k2} < q$, $10^{k3} < q$, $10^{k1+k2+k3} < p$) (column 7, lines 20-27)
- H : hash function
- E : symmetric encipher function (the domain of E is all positive integers)

- a cipher-text generation and transmission step of selecting random numbers $\alpha = \alpha_1 || \alpha_2$ ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$, where |x| is the number of digits of x),
- selecting a random number $r \in Z_{q,}$ calculating:

  $u_1 = g_1^r$ mod p, $u_2 = g_2^r$ mod p, $v = g_1$^ α_1 c^r $d^{\alpha r}$ mod p, K = H(h^r mod p)
- transmitting the ciphertext (u_1, u_2, v, C) (column 8, lines 24-35);
- generating a ciphertext C of transmission data m by: $C = E_K(\alpha_1||\alpha_2||m)$ (column 12, lines 1-35) by using a symmetric cryptographic function, and
- transmitting (u_1, u_2, v, C) as the ciphertext (column 8, lines 24-35);
- a ciphertext reception and decipher step of calculating K' = H(u_1^z mod p) by using the secret key, calculating from the received ciphertext, α_1', α_2' ($|\alpha_1'| = k_1$, $|\alpha_2'| = k_2$) which satisfy: $\alpha_1'||\alpha_2'||m' = D_{K'}(\ C\ )$

- and if the following is satisfied:

  $(g_1\hat{}\alpha_1')(u_1\hat{}(x_1+\alpha'y_1))(u_2\hat{}(x_2+\alpha'y_2))\equiv v \pmod p$

  outputting m' as the deciphered results (where $\alpha' = \alpha_1' \mid\mid \alpha_2'$, whereas if not satisfied, outputting as the decipher results the effect that the received cipher-text is rejected (column 8, lines 36-67).

Cramer et al. disclose generating a secret-key using five exponent numbers (x_1, x_2, y_1, y_2, $z \in Z_q$), generating a public-key, and transmitting a cipher-text (u_1, u_2, e, v). Furthermore, Cramer et al. teach generating extended private key and public key (column 4, lines 19-45). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate the secret key by modifying Cramer et al.'s generating step. One of ordinary skill in the art would have been motivated to do so to increase the security of the cryptographic scheme (Cramer et al., column 4, lines 19-67).

Regarding claim 15, Cramer et al. do not disclose expressly wherein the public-key is generated by a receiver and is made public. However, Examiner takes Official Notice that having a receiver generating a public-key and making it public is conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to have a receiver generate a public-key and make it public since Examiner takes Official Notice that having a receiver generating a public-key and making it public is conventional and well known.

Regarding claim 16, Cramer et al. teach wherein in said ciphertext transmission step, the random numbers α_1 , α_2 ($\alpha_1 \in X_1$, $\alpha_2 \in X_2$) and $r \in Z_q$ are selected beforehand and the u_1, u_2, e, and v are calculated and stored beforehand (column 7, lines 40-67, column 8, lines 1-22).

Regarding claim 17, Cramer et al. teach wherein in said ciphertext transmission step, the random numbers α_1 , α_2 ($|\alpha_1|= k_1$, $|\alpha_2| = k_2$), and $r \in Z_q$ are selected beforehand and the u_1, u_2, e, and v are calculated and stored beforehand (column 7, lines 40-67, column 8, lines 1-22).

Regarding claim 18, Cramer et al. teach a cryptographic communication method comprising: a key generation step of generating a secret-key:

- $x_1, x_2, y_1, y_2 \in Z_q$ (column 7, lines 10-19),
- sk : (asymmetric cryptography) decipher key
- and a public-key:
    - G : finite (multiplicative) group
    - q: prime number (the order of G),
    - $g_1,g_2 \in G$ (column 6, lines 65-67, column 7, lines 1-10),
    - c= g_1^x_1 g_2^x_2, d= g_1^y_1 g_2^y_2,
    - $\pi : X_1 \times X_2 \times M \rightarrow \mathrm{Dom}(E)$: one-to-one mapping, (Dom (E) is the domain of the function E)
    - $\pi^{-1} : \mathrm{Im}(\pi) \rightarrow X_1 \times X_2 \times M$ (column 7, lines 20-27)
    - $E_{pk}(.)$: (asymmetric cryptography) encipher function (column 12, lines 1-35)

- where the group G is a partial group of the group G', X_1 and X_2 are an infinite set of positive integers which satisfy: $\alpha_1 \| \alpha_2<q$ (for every $\alpha_1 \in X_1$, for every $\alpha_2 \in X_2$) where M is a plaintext space;
- a cipher-text generation and transmission step of selecting random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in Z_q$, calculating: $u_1=g_1^r$, $u_2=g_2^r$, $v=g_1{}^\wedge\ \alpha_1 c^r\ d^{\alpha r}$ (column 7, lines 55-67, column 8, lines 1-22) where $\alpha = \alpha_1 \| \alpha_2$, generating a ciphertext C of transmission data m by: $e = E_{pk}(\pi(\alpha_1,\alpha_2,m))$ (column 12, lines 1-35) by using an asymmetric cryptographic function E_{pk}, and transmitting (u_1, u_2, e, v) as the ciphertext (column 8, lines 24-35); and
- a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α_1', α_2', m' ($\alpha_1' \in X_1$, $\alpha_2' \in X_2$, $m' \in M$) which satisfy: $\pi(\alpha_1', \alpha_2', m') = D_{sk}(e)$ (column 8, lines 36-67, column 9,lines 1-67, column 10, lines 1-67)
- and if the following is satisfied:

  $(g_1{}^\wedge\alpha_1')(u_1{}^\wedge(x_1+ \alpha' y_1))(u_2{}^\wedge(x_2+ \alpha' y_2))=v$
- where $\alpha' = \alpha_1' \| \alpha_2'$
- outputting m' as the deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected (column 8, lines 36-67).

Cramer et al. disclose generating a secret-key using five exponent numbers (x_1, x_2, y_1, y_2, $z \in Z_q$), generating a public-key, and transmitting a cipher-text (u_1, u_2, e, v). Furthermore, Cramer et al. teach generating extended private key and public key (column 4, lines 19-45). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate the secret key by modifying Cramer et al.'s generating step. One of ordinary skill in the art would have been motivated to do so to increase the security of the cryptographic scheme (Cramer et al., column 4, lines 19-67).

Regarding claim 19, Cramer et al. teach a cryptographic communication method comprising: a key generation step of generating a secret-key:

- $x_1, x_2, y_1, y_2 \in Z_q$ (column 7, lines 10-19),
- sk : (asymmetric cryptography) decipher key, and
- a public-key:
    - p, q: prime number (q is a prime factor of p-1),
    - $g_1, g_2 \in Z_p$: $ord_p(g_1) = ord_p(g_2) = q$ (column 6, lines 65-67, column 7, lines 1-10),
    - $c= g_1$^x_1 g_2^x_2 mod p, $d= g_1$^y_1 g_2^y_2 mod p,
    - k_1 , k_2 : positive constant ($10^{k1+k2} < q$) (column 7, lines 20-27)
    - $E_{pk}(.)$: (asymmetric cryptography) encipher function (column 12, lines 1-35)

- a cipher-text generation and transmission step of selecting random numbers $\alpha = \alpha_1 \| \alpha_2$ ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$ where $|x|$ is the number of digits of x); selecting a random number $r \in Z_{q,}$ calculating:

  $u_1 = g_1^r \bmod p$, $u_2 = g_2^r \bmod p$, $v = g_1\hat{}\ \alpha_1 c^r\ d^{\alpha r} \bmod p$

- generating a ciphertext C of transmission data m (positive integer) by:

  $e = E_{pk}(\alpha_1 \| \alpha_2 \| m)$ (column 12, lines 1-35)

- by using the secret key, and transmitting (u_1, u_2, e, v) as the ciphertext (column 8, lines 24-35); and

- a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α_1', α_2', m' ($|\alpha_1'| = k_1$, $|\alpha_2'| = k_2$, m' is appositive integer) which satisfy: $\alpha_1' \| \alpha_2' \| m' = D_{sk}(e)$ (column 8, lines 36-67, column 9,lines 1-67, column 10, lines 1-67)

- and if the following is satisfied:

  $(g_1\hat{}\alpha_1')(u_1\hat{}(x_1 + \alpha' y_1))(u_2\hat{}(x_2 + \alpha' y_2)) = v \pmod p$

- where $\alpha' = \alpha_1' \| \alpha_2'$

- outputting m' as the deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received cipher- text is rejected (column 8, lines 36-67).

Cramer et al. disclose generating a secret-key using five exponent numbers (x_1, x_2, y_1, y_2, $z \in Z_q$), generating a public-key, and transmitting a cipher-text (u_1, u_2, e, v). Furthermore, Cramer et al. teach generating extended private key and public key (column 4, lines 19-45). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate the secret key by modifying Cramer et al.'s generating step. One of ordinary skill in the art would have been motivated to do so to increase the security of the cryptographic scheme (Cramer et al., column 4, lines 19-67).

Regarding claim 20, Cramer et al. do not disclose expressly wherein the public-key is generated by a receiver and is made public. However, Examiner takes Official Notice that having a receiver generating a public-key and making it public is conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to have a receiver generate a public-key and make it public since Examiner takes Official Notice that having a receiver generating a public-key and making it public is conventional and well known.

Regarding claim 21, Cramer et al. teach wherein in said ciphertext transmission step, the random numbers α_1 , α_2 ($\alpha_1 \in X_1$, $\alpha_2 \in X_2$) and $r \in Z_q$ are selected beforehand and the u_1, u_2, and v are calculated and stored beforehand (column 7, lines 40-67, column 8, lines 1-22).

Regarding claim 22, Cramer et al. teach wherein in said ciphertext transmission step, the random numbers α_1 , α_2 ($|\alpha_1|= k_1$, $|\alpha_2| = k_2$), and $r \in Z_q$ are selected beforehand and the u_1, u_2, and v are calculated and stored beforehand (column 7, lines 40-67, column 8, lines 1-22).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US Patent Number: 6,081,598 to Dai, for "a cryptography system improves the decryption speed in the RSA algorithm by taking advantage of certain subgroups of Z_n*. The cryptography system employs a new family of trapdoor permutations based on exponentiation in subgroups of Z_n*".

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 8:30 am - 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DGC